BLACK BOX NETWORK SERVICES

LWN602A
LWN602AE
LWN602HA
LWN602HAE
LWN600VMA
LWN600CM-1
LWN600CM-3
LWN602WA

SmartPath™ OS and SmartPath EMS VMA 4.1r5 Release Notes

v4.1r5 Release Notes

SmartPath provides the speed, range, security, adapability, and mangeability to replace wired networks at an enterprise level.

Customer Support Information

Order toll-free in the U.S.: Call 877-877-BBOX (outside U.S. call 724-746-5500)
FREE technical support 24 hours a day, 7 days a week: Call 724-746-5500 or fax 724-746-0746
Mailing address: Black Box Corporation, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: www.blackbox.com • E-mail: info@blackbox.com

Black Box Release Notes

Versions: SmartPath OS and SmartPath EMS VMA 4.1r5 Releases

Platforms: SmartPath AP Series, SmartPath EMS VMA, High Capacity SmartPath EMS VMA, SmartPath EMS VMA Online, SmartPath EMS VMA Virtual Appliance

Release Date: July 31, 2012

These are the release notes for SmartPath OS 4.1r5 firmware for the SmartPath AP series devices and SmartPath EMS VMA 4.1.r5 software. This release adds support of all Black Box OUIs, and addresses a number of issues, which are described in the "Addressed Issues" section near the end of this document.

New Features and Feature Enhancements

Several new features and feature enhancements have been introduced in the SmartPath OS and SmartPath EMS VMA 4.1 releases. You can read summaries of these features and enhancements below. If there are no entries listed for a particular release, no new major features or feature enhancements were added in that release.

New Features and Enhancements in the 4.1r5 Releases

New Black Box MAC OUI Support: LWN602A, LWN602HA, LWN600VMA, and LWN602WA series devices must be running SmartPath OS 4.1r5 to be able to mesh with access point devices on SmartPath OS 5.1r1.

New Features and Enhancements in the 4.1r4 Releases

Band Steering and Load Balancing Improvements: SmartPath EMS VMA now provides more granular and flexible control over traffic-optimizing features. This is particularly useful for implementations in which there is relatively dense client deployment without dense (that is, overlapping) AP deployment, such as in schools, training facilities, and similar environments. When you create or edit an existing radio profile, you can now find the options that are used specifically to optimize traffic in a new, separate expandable section called Optimizing Management Traffic Settings. In addition, you now have the ability to control to a fine degree how the APs handle band usage and steering.

DHCP Options for Private PSK and RADIUS: SmartPath AP devices can recognize DHCP options from Black Box routers advertising themselves as a private PSK server (DHCP option 229), RADIUS authentication server (DHCP option 230), and RADIUS accounting server (DHCP option 231).

New Features and Enhancements in the 4.1r3 Releases

APs with different OUIs can mesh.

Country Certifications: LWN602A devices have been certified for Brazil.

New Features and Enhancements in the 4.1r2b Releases

Country Certifications: The following new country certifications have been added with the 4.1r2b releases:

- LWN602WA devices are certified for the United Arab Emirates.
- LWN602A devices are certified for China.

New Features and Enhancements in the 4.1r2 Releases

The following are the new and enhanced features being introduced in the SmartPath OS and SmartPath EMS VMA 4.1r2 releases.

Netdump: The netdump feature now includes specifications for VLAN parameters and options for selecting how the bootloader connects to the network. You can now specify an explicit VLAN as well as the native VLAN that the SmartPath AP uses when it boots up after experiencing a system failure. In addition, you can specify whether the SmartPath AP bootloader gets its information from a DHCP server or from static network settings that you specify directly on the Monitor > Access Points > SmartPath APs > cluster_ap > Update Netdump Settings page.

New Features and Enhancements in the 4.1r1 Releases

The following are the new and enhanced features being introduced in the SmartPath OS and SmartPath EMS VMA 4.1r1 releases.

LWN602WA for Outdoor Wi-Fi: The LWN602WA is a new platform for outdoor Wi-Fi deployments. In support of this new device, antenna alignment controls for long-distance transmissions have been added to SmartPath OS as well as settings to adjust for long radio ranges and limit the availability of channels for outdoor use.

Antenna Alignment Tool: The LWN602WA allows you to apply fine adjustments to directional or sector antennas. By entering a simple CLI command, the LWN602WA can be made to send a number of alignment frames to a peer. The responses received contain information regarding the power levels on each end of the link, which you can use to determine how well aligned the link is.

Channel Restriction: You can configure the LWN602WA explicitly to operate as an indoor device or an outdoor device. When it is in outdoor mode, the UNII-1 band becomes unavailable in the FCC regulatory domain in accordance with FCC restrictions, and the UNII-1 and UNII-2 bands become unavailable in the ETSI regulatory domain in accordance with ETSI restrictions. This helps in part to prevent the unintentional use of unauthorized channels.

Selective Multicast Forwarding through GRE Tunnels: SmartPath APs can selectively block or allow broadcast and multicast traffic through GRE tunnels to reduce traffic congestion. You can filter traffic either by using a blacklist to block all broadcast and multicast traffic (or to block all except to a few select destinations) or by using a whitelist to allow all broadcast and multicast traffic (or to allow all except to a few destinations).

Multiple Default Routing: It is now possible to configure multiple Layer 2 routes based on the VLAN ID of a user so that the SmartPath AP can route Layer 2 traffic through different Ethernet interfaces as appropriate. This allows, for example, a guest user on a corporate network segment to access a more appropriate segment for routing to the Internet while the SmartPath AP forwards traffic from an employee on a different VLAN through a different Ethernet interface.

Captive Web Portal Enhancements: The default captive Web portal pages have been redesigned to resize automatically for optimal viewing per device type: smartphone, tablet, and computer monitor. In addition, captive web portals can now support a registration page with buttons linking to various URLs.

IP Multicast Enhancements: To minimize airtime consumption caused by multicast frame transmissions, SmartPath APs can convert multicast to unicast frames when channel use is high or multicast group membership is low. Furthermore, when a SmartPath AP cannot detect any multicast group members among its active clients, it can automatically suppress multicast frame transmissions completely.

LLDP Maximum Power: To avoid SmartPath APs sending Link Layer Discovery Protocol (LLDP) transmissions requesting more power through PoE from the connecting switch than the switch can provide, you can set a maximum power level that SmartPath APs can request in their LLDP advertisements on the Configuration > Advanced Configuration > Network Objects > LLDP/CDP Profiles > New page. By default, the maximum is 15.4 watts.

Changes to Behavior

The following change to default behavior has been introduced in the 4.1r4 releases:

In previous releases, the manual classification of APs as either rogue or friendly only affected the way that SmartPath EMS VMA displayed the APs that managed Black Box APs reported to it. In this release, SmartPath EMS VMA pushes the rogue and friendly classifications to the Black Box APs under its management so that if you enable semi-automatic or automatic mitigation of rogue APs, the mitigator APs will not mitigate any APs classified as friendly. Conversely, the mitigator APs will mitigate any APs manually classified as rogue. As soon as you put an AP in one of the two categories, SmartPath EMS VMA communicates its classification to managed APs. As a result, if you manually classify an AP as rogue and automatic mitigation is enabled, mitigator APs immediately take action to attack the rogue. On the other hand, classifying an AP as friendly immediately cancels any attack currently underway against it.

The following change to default behavior was introduced in the 4.1r3 releases:

- An AP determines whether a detected rogue AP is in its backhaul network by checking its MAC learning table for any entry within a range of 64 addresses above or 64 addresses below the BSSID of the invalid SSID. If it finds an address within that range, it determines the rogue to be in the same network and takes the action specified in the WIPS policy to mitigate it. In previous releases, Black Box included an alternative detection mechanism, but it was removed because it was redundant, more complex to configure, and did not detect devices running Network Address Translation (NAT).

The following changes to default behavior were introduced in the 4.1r2 releases:

- Multicast-unicast conversion is disabled by default. However, if you upgrade from 4.1r1, then the setting will remain set to Auto after the upgrade to 4.1r2.
- SmartPath EMS VMA is enabled as an NTP client by default. Upgrading from 4.0 or 4.1r1 does not change the current configuration.
- SmartPath EMS VMA Online administrators can now change the report polling interval. In previous versions, this can only be done by the admin in the home system.

The following changes to default behavior were introduced in the 4.1r1 releases:

- To accommodate large, flat networks whose broadcast domain includes many hosts, the Address Resolution Protocol (ARP) table capacity has been increased from 256 to 8192 entries.
- The beacon period range has been increased from 25–1000 TUs (time units) to 40–3500 TUs.
- The policing rate limit for Black Box Class 5 traffic (video) in the default QoS profile has been changed from 50,000 kbps to 100,000 kbps.

Automatically Discovering the CAPWAP Server

SmartPath APs and SmartPath EMS VMA communicate with one another through Control and Provisioning of Wireless Access Points (CAPWAP). SmartPath APs act as CAPWAP clients and SmartPath EMS VMA acts as a CAPWAP server. SmartPath APs can form a CAPWAP connection with SmartPath EMS VMA in any of the following ways:

- When SmartPath APs are in the same Layer 2 broadcast domain as a SmartPath EMS VMA appliance or SmartPath EMS VMA Virtual Appliance, the SmartPath APs broadcast CAPWAP Discovery Request messages to discover SmartPath EMS VMA and establish a secure connection with it automatically.
- If there is no SmartPath EMS VMA in the same broadcast domain but the SmartPath APs can reach the SmartPath EMS VMA Online staging server—and MAC address or serial number entries for the SmartPath APs have already been added to the SmartPath EMS VMA Online access control list (ACL)—then they can form secure CAPWAP connections with the staging server. From there, an administrator can assign the connected SmartPath APs to a virtual SmartPath EMS VMA at the cluster site or to a SmartPath EMS VMA appliance—virtual or otherwise—at another site.
- Finally, SmartPath APs and a local SmartPath EMS VMA might be in different subnets and the SmartPath APs either cannot reach SmartPath EMS VMA Online or they can but they are not listed in the ACL (perhaps because they are not included in any SmartPath EMS VMA Online account). In this case, the SmartPath APs cannot discover SmartPath EMS VMA by broadcasting CAPWAP Discovery Request messages, nor can they reach the staging server. To enable the SmartPath APs to form a CAPWAP connection to SmartPath EMS VMA, you can use one of the following methods to configure SmartPath APs with the SmartPath EMS VMA domain name or IP address or configure them so that they can learn it through DHCP or DNS settings. When SmartPath APs have the IP address of the CAPWAP server, they then send unicast CAPWAP Discovery Request messages to that address.

Log in to the CLI on each SmartPath AP and enter the IP address of the CAPWAP server with the following command:

```
capwap client server name
```

Configure the DHCP server to supply the domain name of the CAPWAP server as DHCP option 225 or its IP address as option 226 in its DHCPOFFER. (If you use a domain name, the authoritative DNS server for that domain must also be configured with an "A" record that maps the domain name to an IP address for the CAPWAP server.) SmartPath APs request DHCP option 225 and 226 by default when they broadcast DHCPDISCOVER and DHCPREQUEST messages.

The IP address of the CAPWAP server must be accessible from the SmartPath AP VLAN. If you need to change the DHCP option number (perhaps because another custom option with that number is already in use on the DHCP server), enter this command with a different option number for the variable "<number>": interface mgt0 dhcp client option custom SmartPath EMS VMA <number> { ip | string }

If SmartPath EMS VMA continues to use its default domain name ("SmartPath EMS VMA") plus the name of the local domain to which it and the SmartPath APs belong, configure an authoritative DNS server with an "A" record that resolves "SmartPath EMS VMA.<local_domain>" to an IP address. If SmartPath APs do not have an IP address or domain name configured for the CAPWAP server and do not receive an address or domain name returned in a DHCP option, then they try to resolve the domain name to an IP address.

When a SmartPath AP goes on-line for the first time without any specific CAPWAP server configuration entered manually or received as a DHCP option, it progresses through the cycle of CAPWAP connection attempts shown below. (Note that the "SmartPath EMS VMA" in the upper semicircle can be either a physical SmartPath EMS VMA appliance or SmartPath EMS VMA Virtual Appliance.)

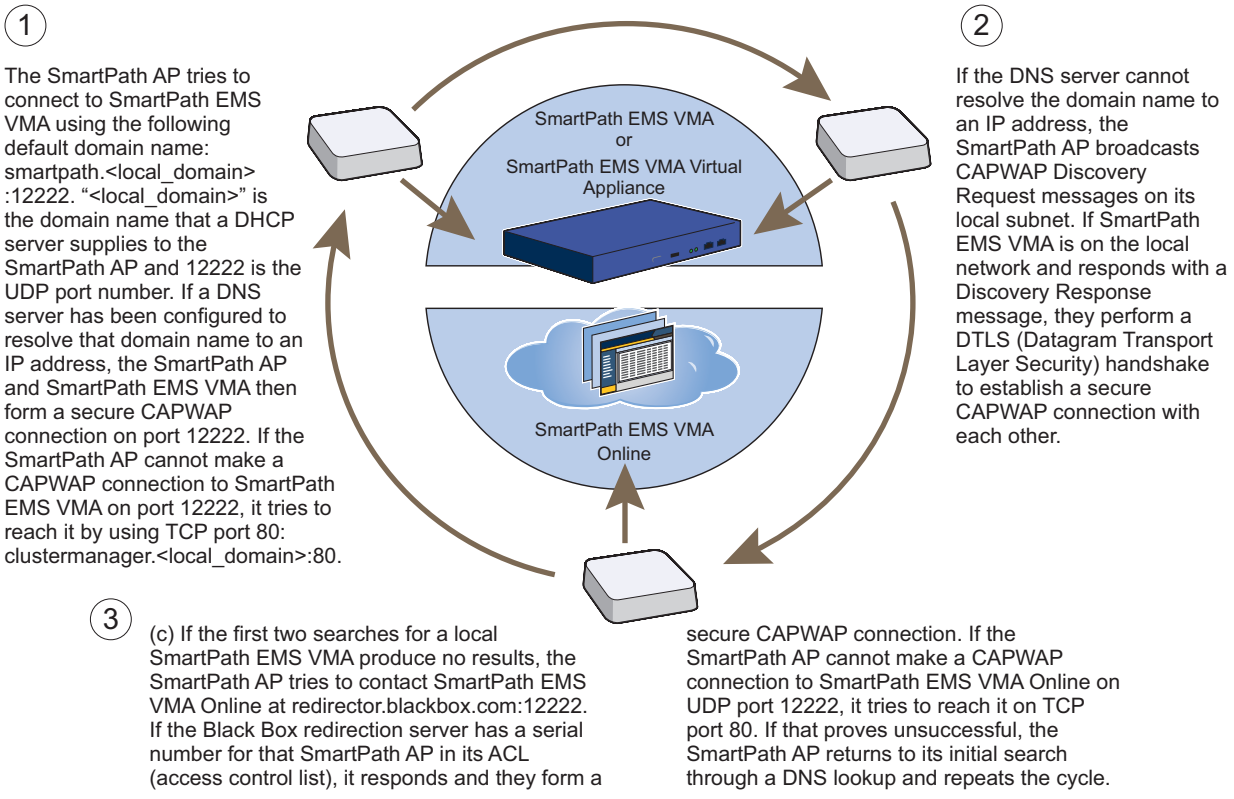
1
The SmartPath AP tries to connect to SmartPath EMS VMA using the following default domain name: smartpath.<local_domain> :12222. "<local_domain>" is the domain name that a DHCP server supplies to the SmartPath AP and 12222 is the UDP port number. If a DNS server has been configured to resolve that domain name to an IP address, the SmartPath AP and SmartPath EMS VMA then form a secure CAPWAP connection on port 12222. If the SmartPath AP cannot make a CAPWAP connection to SmartPath EMS VMA on port 12222, it tries to reach it by using TCP port 80: clustermanager.<local_domain>:80.
SmartPath EMS VMA or SmartPath EMS VMA Virtual Appliance
SmartPath EMS VMA Online
2
If the DNS server cannot resolve the domain name to an IP address, the SmartPath AP broadcasts CAPWAP Discovery Request messages on its local subnet. If SmartPath EMS VMA is on the local network and responds with a Discovery Response message, they perform a DTLS (Datagram Transport Layer Security) handshake to establish a secure CAPWAP connection with each other.
3
(c) If the first two searches for a local SmartPath EMS VMA produce no results, the SmartPath AP tries to contact SmartPath EMS VMA Online at redirector.blackbox.com:12222. If the Black Box redirection server has a serial number for that SmartPath AP in its ACL (access control list), it responds and they form a secure CAPWAP connection. If the SmartPath AP cannot make a CAPWAP connection to SmartPath EMS VMA Online on UDP port 12222, it tries to reach it on TCP port 80. If that proves unsuccessful, the SmartPath AP returns to its initial search through a DNS lookup and repeats the cycle.

Figure 1. Discovering the CAPWAP server.

If the SmartPath AP forms a CAPWAP connection with the Black Box redirection server and its serial number has been entered in an ACL, the redirection server automatically redirects its CAPWAP connection to the corresponding SmartPath EMS VMA Online (virtual SmartPath EMS VMA). The redirection server does this by sending the SmartPath AP the SmartPath EMS VMA domain name or IP address as its new CAPWAP server and the name of the appropriate virtual SmartPath EMS VMA. If the SmartPath AP is currently using HTTP, the redirection server includes the configuration needed for it to continue using it. Similarly, if the SmartPath AP is configured to access the public network through an HTTP proxy server, the redirection server saves the relevant settings on the SmartPath AP so it will continue using the HTTP proxy server when connecting to SmartPath EMS VMA.

If the staging server does not have the SmartPath AP serial number, then the ACL on the staging server ignores the CAPWAP connection attempts, and the SmartPath AP repeats the connection cycle shown on the previous page.

Troubleshooting the Initial SmartPath AP CAPWAP Connection to SmartPath EMS VMA Online

As explained in the previous section, when you connect a SmartPath AP to the network and power it on, it first tries to connect to a local SmartPath EMS VMA. If it cannot do that, the SmartPath AP automatically tries to connect to the staging server. The staging server checks if the serial number of the SmartPath AP is listed in its ACL—which should be the case as Black Box enters the serial numbers of newly purchased SmartPath APs in the appropriate ACL as part of the sales process. If the ACL contains the SmartPath AP serial number, the staging server then redirects the SmartPath AP to the correct SmartPath Virtual Enterprise Management System (VEMS), where the SmartPath AP appears on the Monitor > Access Points > SmartPath APs page. Log in to your account, click SmartPath EMS VMA Online and navigate to the SmartPath APs page. If you do not see the SmartPath AP listed there, take the following steps to resolve the situation:

NOTE: Depending on network conditions and firewall policies, it can sometimes take up to ten minutes for a SmartPath AP to connect to the staging server and be redirected to the SmartPath EMS VMA Online VEMS to which it belongs. Be sure to give the SmartPath AP enough time to complete the connection process before proceeding.

1. Click "Staging Server > Monitor > SmartPath AP Access Control List," and check if the SmartPath AP serial number is listed there.

2. If the serial number is absent from the ACL, do the following:

2.1 Click "Enter," type the serial number, and then click "Save."

If an error message appears stating that the serial number already exists in the system, contact Black Box Technical Support for further assistance.

2.2 Check if the SmartPath AP now appears on the Monitor > Access Points > SmartPath APs page in SmartPath EMS VMA Online. Remember that it might take up to ten minutes for it to complete the connection process.

2.3 If the SmartPath AP still does not appear on the SmartPath APs page, power the SmartPath AP off, wait five seconds, power it back on, and then check the SmartPath APs page again.

2.4 If the SmartPath AP still does not appear on the SmartPath APs page, check that the SmartPath AP can access the Internet and that any firewall between it and the staging server allows outbound traffic using either UDP 12222 or TCP 80.

If the SmartPath AP connects and appears on the SmartPath APs page in your SmartPath EMS VMA Online VEMS, you have successfully resolved the issue and can stop troubleshooting. If not, continue to the next step.

3. If the serial number of the SmartPath AP is listed in the ACL on the staging server but the SmartPath AP does not appear on the SmartPath APs page in SmartPath EMS VMA Online, first follow steps 2.3 and 2.4 (if you have not already done so). If it still does not appear, the SmartPath AP might be redirected to the SmartPath EMS VMA Online home system, which can occur if the CAPWAP server name on the SmartPath AP was accidentally misconfigured. To reassign it your VEMS, do the following:

3.1 In SmartPath EMS VMA Online, click "Configuration > Advanced Configuration > SmartPath AP Auto Provisioning > SN Management > Scan SN", type the 14-digit serial number for the SmartPath AP, and then click "Save." After that, click "Cancel" to close the Imported SmartPath AP Serial Numbers dialog box.

3.2 On the SmartPath AP Auto Provisioning page, click "New," enter the following, and then click "Save:"

Enable SmartPath AP Auto Provisioning: (select)

SmartPath AP Model: Choose the appropriate SmartPath AP model from the drop-down list.

Apply access control: (select)

Imported SmartPath AP Serial Numbers: (select)

Select the serial number that you just entered in the previous step and click the right arrow (>) to move it from the Available Serial Numbers column to the Selected Serial Numbers column.

3.3 Reboot the SmartPath AP to reset its CAPWAP state to Discovery. When it contacts the staging server this time, SmartPath EMS VMA Online will apply the access control defined in the automatic provisioning configuration and redirect the SmartPath AP to your VEMS.

Upgrading SmartPath EMS VMA Software and SmartPath OS Firmware

Black Box supports upgrading to the 4.1r5 SmartPath EMS VMA software and SmartPath OS firmware from the SmartPath EMS VMA and SmartPath OS 3.5r1 releases or later. If your systems are running images earlier than 3.5r1, follow the steps in the 3.5r1 Black Box release notes to upgrade SmartPath EMS VMA software and SmartPath OS firmware to 3.5r1 first before upgrading them to 4.1r5.

Step 1: Upgrade 3.5r1 or later to 4.1r5

When upgrading SmartPath EMS VMA software and SmartPath OS firmware to 4.1r5, upgrade SmartPath EMS VMA first and then the SmartPath APs second. The full upgrade procedure is outlined below.

From To

SmartPath EMS VMA 3.5r1 or later ——————————————————> 4.1r5

Upgrade to SmartPath EMS VMA 4.1r5

SmartPath OS 3.51 or later ——————————————————> SmartPath OS 4.1r5

Use SmartPath EMS VMA running SmartPath EMS VMA 4.1r5
to upgrade managed SmartPath APs to SmartPath OS 4.1r5

1. Save the following files to a directory on your management system or SCP server:

   SmartPath EMS VMA 4.1r5 software file

   SmartPath OS 4.1r5 firmware file

2. Log in to SmartPath EMS VMA running 3.5r1 or later, upload the SmartPath OS 4.1r4 firmware file and the SmartPath EMS VMA 4.1r5 software file, and then reboot SmartPath EMS VMA to activate its new software.

3. Log back in to SmartPath EMS VMA, which is now running 4.1r5, and upload SmartPath OS 4.1r5 from SmartPath EMS VMA to all managed SmartPath APs, and then reboot them to activate their new firmware.

Step 2: Reload the SmartPath AP Configurations

1. Check that the firmware upgrade is complete (see Monitor > SmartPath AP Update Results).

2. Upload the full configurations from SmartPath EMS VMA to the SmartPath AP, and then reboot them to activate the 4.1r5-compatible configurations.

NOTE: SmartPath EMS VMA running SmartPath EMS VMA 4.1r5 can support clusters running SmartPath OS 3.5r1 through 4.1r5. Based on the SmartPath OS version that the members of each cluster are using, SmartPath EMS VMA generates different configurations. Therefore, it is necessary to activate the SmartPath OS 4.1r5 firmware on managed SmartPath APs before updating their configurations so that the updated configurations will use the new 4.1r5 format.

Documentation

Technical documentation for installing and configuring Black Box APs and SmartPath EMS VMA is available in the Black Box User's Manual. This guide includes both hardware- and software-specific information for both types of devices.

In addition, there are online CLI reference guides that provide the syntax and explanations for every command in the CLI. They also include information on accessing the CLI through console, Telnet, and SSH connections, tips on using the CLI, and some keyboard shortcuts.

Known Issues

The following are known issues at the time of the SmartPath OS and SmartPath EMS VMA 4.1r5 releases:

Known Issues in SmartPath EMS VMA 4.1r5

12002

Exporting the event log (Monitor > Events > Export) only includes events listed on the currently active page.

Workaround: Change Items per page to 500 to maximize the number of log entries per page and minimize the total number of pages that must be individually exported, and then click Export. If necessary, advance to subsequent pages and export them individually as well.

11841

The Client SLA Compliance and SmartPath AP SLA Compliance widgets on the Home > Dashboard page sometimes continue to show clients and SmartPath APs as noncompliant after they return to a compliant state.

11833

A Black Box appliance running SmartPath EMS VMA without GuestManager does not send traffic out its LAN interface to the default gateway even when the default gateway is in the same subnet as the LAN interface. (An appliance with an active GuestManager license only supports the MGT interface, so this issue does not apply in that case.)

Workaround: Connect just the MGT interface to the network and set the default gateway in its subnet.

10777

Active wireless clients cannot be shown on a topology map when the "Calibrate heat maps" option is enabled in the global settings dialog box for topology maps.

Workaround: Disable the Calibrate heat maps option.

Addressed Issues

The following known major issues in previous SmartPath OS and SmartPath EMS VMA releases have been addressed in 4.1. If there are no entries listed for a particular release, no previously known major issues were addressed in that release.

Addressed Issues in SmartPath OS 4.1r5

18175

When performing an SNMP walk, a SmartPath AP erroneously reports that the operational state of eth1 is up even when no cable is physically connected to that interface.

17302, 17209

Black Box devices responded to SNMP queries with erroneous information regarding traffic volume and client airtime usage.

17195

Black Box devices did not support more than 7250 private PSK rotations.

16893

Black Box devices did not prevent upload attempts of SmartPath OS image files containing special characters, which would cause the upload attempts to fail.

16872, 16743, 16691

SmartPath AP devices occasionally restarted or experienced high CPU usage after extended periods of use.

16726

Native Windows® 7 RADIUS supplicants did not fail over to a backup RADIUS server after the primary server became unreachable.

16577

When CDP was enabled on Black Box APs that were connected to Cisco® switches running an older version of CDP code, users could sometimes be disconnected from the APs.

15910

SmartPath devices configured as L2 VPN servers were prone to restart after extended periods of use.

Addressed Issues in SmartPath OS 4.1r4

16745

When ALG packet processing was enabled on an AP and it received a packet with IP options set, the extra packet length could trigger the AP to reboot.

16710

When Black Box devices sent RADIUS messages to a backup RADIUS server because the primary server was unavailable, the NAS-IP-Address attribute was included twice in Access-Request messages, which the server rejected.

16697

When a client had a DHCP lease that was greater than 24 days, the Black Box device to which it was connected marked the client's lease as expired and displayed a network health score of 0 although the client still had a valid lease.

16612

When executing an Active Directory/LDAP connectivity test, a Black Box device always stripped the domain name from user@ domain before sending the message to the LDAP server which would cause the test to fail for those LDAP servers that required the full user name.

16558

Client throughput on an SSID using 802.1X authentication was considerably lower than on one using PSK.

16464

Clients generating large numbers of IP sessions could cause a Black Box device to reboot.

16351

Black Box devices were unable to support wireless clients using supplicants such as Cisco® ACU and Dell® Broadcom if they specified authentication type 128 for LEAP authentication.

16288

Aligning antennas on a SmartPath mesh point with the exec antenna-alignment command disrupted the mesh link.

16158

If user profile reassignment was applied to a client and it then roamed to another device, the new device would apply the SSID-assigned user profile instead of the reassigned profile.

16045

If clients sent a large number of HTTP or HTTPS requests to the mgt0 interface on a SmartPath device, it could become overloaded and reboot.

15931

Older versions of ASUS® Skype® phones could not make wireless connections to APs.

Addressed Issues in SmartPath OS 4.1r3

16337

When the admin performed a database backup and a software upgrade on SmartPath EMS VMA Online, the RADIUS objects were not restored properly.

15919

High CPU utilization on the SmartPath AP sometimes disrupted CAPWAP functionality, after which the AP could not reestablish the CAPWAP connection and required a reboot.

Addressed Issues in SmartPath OS 4.1r2b

15972

SmartPath OS private PSK generation was incorrect for Daylight Savings Time in time zones in the Southern Hemisphere.

Addressed Issues in SmartPath OS 4.1r2a

15911

If a SmartPath AP successfully performed a backhaul failover from eth0 to a wireless interface and then the wireless interface lost its link, the SmartPath AP would be unable to fail back to eth0 later when its Ethernet link was restored.

15726

When attempting to upgrade a SmartPath AP to SmartPath OS 4.1r1, some SmartPath APs did not load the 4.1r1 version of SmartPath OS when they rebooted but continued running the previous SmartPath OS version.

Addressed Issues in SmartPath OS 4.1r2

15751

Automatic multicast-to-unicast conversion caused MacBookPro® not to work with Bonjour® printers.

15543

SpectraLink® 8440 phones failed to authenticate when the SSID was configured for WPA/WPA2 PSK.

15390

When authenticating using Kerberos, some SmartPath APs failed the authentication handshake.

Addressed Issues in SmartPath OS 4.1r1

14879

When connected to Godex® 802.11 b/g wireless barcode printers, SmartPath APs running 4.0r1 and 4.0r1a SmartPath OS code experienced continuous reboots.

14874

Under certain circumstances, the flash log could become inundated with input/output control messages, which in turn sometimes caused the SmartPath AP to reboot repeatedly.

14853

Although a user name can be up to 32 characters long, the names of roaming users shown in the roaming cache were truncated to 16 characters.

14839

When a SmartPath AP RADIUS server integrated with an eDirectory user database, the account policy check was not performed although it was enabled.

14639

It was not possible to do an LDAP search on Open Directory if the user attribute was anything other than "CN."

14467

A SmartPath AP functioning as a mesh point could not use DHCP to receive its network setting through a SmartPath AP portal.

14411

Intel® 2200BG wireless clients were unable to complete the 802.11 authentication process with SmartPath APs.

14351

If you enabled LLDP (Link Layer Discovery Protocol) transmissions on a SmartPath AP, it requested the connecting switch to extend its power through PoE to 17.5 W (watts). However, Cisco 802.af-compliant switches do not support that level, and cut the power supplied to the SmartPath AP, which caused it to reboot continuously.

13983

Alcatel-Lucent OmniTouch™ 8118/8128 WLAN Handsets were unable to form associations with SmartPath APs.

Addressed Issues in SmartPath EMS VMA 4.1r5

18226

When SmartPath EMS VMA pushed permanent private PSK users to managed devices, it did not save them to Flash so that they would be lost the next time the device rebooted.

18187

If a SmartPath EMS VMA node host name contained uppercase characters, it was not possible to perform a switchover operation.

17557

The start and end times for private PSK users became incorrect after Daylight Savings Time took effect.

17461

Different default RSSI validity periods for Black Box location servers on different platforms caused the configuration audit to show a mismatch for SmartPath AP devices.

17449

If a user name contained "@", the user could not be authenticated against user databases on Black Box devices.

17441

After upgrading to 4.1r3, it was not possible to push configurations to managed devices if the configuration included any RADIUS objects.

17397

SmartPath EMS VMA running 4.1r3 or 4.1r4 could not manage APs running 3.5r5.

17334

Heat maps and the interfaces of managed devices were not displayed correctly in exported Black Box Planning Reports.

17172

Upgrading SmartPath EMS VMA from Express to Enterprise mode caused the AAA user directory settings to be lost.

17027

SmartPath EMS VMA sometimes did not display the wifi1 channel and power levels because of a mismatch between the fields reported by SmartPath OS and the fields displayed by SmartPath EMS VMA.

17026

When there were more than 1000 entries in a user OU in Active Directory, SmartPath EMS VMA was unable to display all the entries and would not display the User Profile field, making it impossible to map an OU to a user profile.

16963

If the private PSK user start time was later than the current time set on SmartPath EMS VMA, incorrect key lifetimes and user start times would be generated.

16962

When there were more 500 managed devices, it was not possible to enter a client MAC address in the Client Monitor tool when the Client Location and Associated Device were both set as "All."

16823

If you included a space after the last digit when entering an IP address in an IP Address field, SmartPath EMS VMA pushed the address with that space to its managed devices, causing the configuration upload to fail.

16453

If an admin attempted to view an SSID that was disabled for a specific device, SmartPath EMS VMA displayed a "Permission denied" error message.

Addressed Issues in SmartPath EMS VMA 4.1r4

16718

(SmartPath EMS VMA Online) When APs on one floor in a building had mesh links with APs on another floor, clicking the interference checkbox above the topology map for one of the floors displayed the "Calculating interference map…" message but never displayed the interference map.

16638

It was not possible to change the idle timeout for automatically clearing inactive, dynamically learned MAC addresses from the MAC learning table for an Ethernet interface in bridge-access mode.

16612

When executing an Active Directory/LDAP connectivity test, a Black Box device always stripped the domain name from user@ domain before sending the message to the LDAP server which would cause the test to fail for those LDAP servers that required the full user name.

16560

An admin with super user privileges logged in to SmartPath EMS VMA using RADIUS authentication could not run reports.

16436

Updating SmartPath EMS VMA to one of the previous releases caused it to remove the domain name from the Web Server Domain Name field in the Optional Advanced Configuration section on the Configuration > Advanced Configuration > Authentication > Captive Web Portals page.

16334

Black Box devices did not recognize all Apple® OUIs properly.

15858

The following issues with third-party certificates have been resolved:

- An intermediate CA certificate was not recognized as the signing certificate for a server certificate unless you first merged it with the appropriate root CA certificate in one .pem file and uploaded the combined file to SmartPath EMS VMA.

- Certificates with special characters such as "(" and ")" could be imported into SmartPath EMS VMA but could not be uploaded to managed Black Box APs because SCP rejected the special characters.
- SmartPath EMS VMA permitted you to upload a CA certificate to an AP even though it did not match the server certificate.
- After saving AAA server settings once, a certificate error appeared whenever an admin tried to edit and save it again, even without making any changes.

Addressed Issues in SmartPath EMS VMA 4.1r2

15828

When using RADIUS for SmartPath EMS VMA administrator authentication, User Manager operators were unable to log in.

15501

SmartPath EMS VMA Online displayed no spectrum analysis data during the analysis process.

15459

After updating to 4.1r1, filters that were previously configured on the Monitor > SmartPath APs page no longer worked properly.

15454

SmartPath EMS VMA incorrectly displayed no aggregate data usage in the dashboard, despite individual SmartPath APs confirming individual data usage.

15363

SmartPath EMS VMA could sometimes become overloaded with rogue detection and mitigation reports, causing it to reboot.

15191

When an Online Planner account expired, it displayed a request for an entitlement key but did not allow the admin to enter it.

15050

SmartPath EMS VMA did not list or allow the creation of SSIDs after update from 3.5r4 evaluation version to 4.1r1.

15023

If an automatically generated private PSK user group was created with a private PSK rotation interval greater than 24 days, no local users were able to be created when enabling automatic creation and rotation of private PSK users and their keys.

15022

When the administrator downloaded the tech data from a SmartPath AP, the downloaded file was unable to retrieve some information.

14935

If SmartPath APs were configured with the name of a building instead of the name of a map (snmp location <string>), SmartPath EMS VMA did not display the SmartPath APs even though they had successfully formed a CAPWAP connection with SmartPath EMS VMA.

14871

After restoring a backed up SmartPath EMS VMA database, the settings to forward selective multicast traffic through GRE tunnels were lost.

14609

Some User Manager operators did not receive appropriate write permissions after logging in.

14410

RADIUS server authentication failed because required fields were missing from the Access-Request packet.

Addressed Issues in SmartPath EMS VMA 4.1r1

15101

When the time zone for the SmartPath EMS VMA system was different from that for a private PSK user group, the private PSKs that SmartPath EMS VMA automatically generated were different from those that SmartPath APs generated.

14635

SmartPath EMS VMA was unable to download SmartPath OS images for the SmartPath AP platforms from the Black Box update server.

14609

If private PSK user accounts in one VEMS expired, a User Manager operator in another VEMS might not have been able to create any more user accounts.

14596

It was not possible for a SmartPath AP to join an Active Directory domain if its domain admin password included either a percent character (%) or an ampersand (&).

14583

If the validity period for a SmartPath EMS VMA-signed server certificate was more than 20 years, saving the AAA server settings would cause an error that the server certificate had not been signed by the SmartPath EMS VMA CA certificate.

14567

When multiple automatically generated private PSK user accounts with varying validity periods were assigned to a User Manager operator, the operator would be unable to create user accounts.

14555

Account lookups for users with the same name in different Active Directory domains would fail.

14465

Applying two OUs or user group names to the same user profile in an AAA User Directory Settings profile produced a configuration error.

14402

Although a captive Web portal providing private PSK self-registration must be configured to use external DHCP and DNS servers, SmartPath EMS VMA allowed the admin to select the internal servers running on the SmartPath AP.

14382

In SmartPath EMS VMA 4.0r1, you could not clone VEMSs containing SSIDs if they had been configured in an earlier version of code.

14378

After retrieving the baseDN for an Active Directory database once, the Retrieve Directory Information button was no longer displayed on the AAA User Directory Settings page, making it difficult for an admin to rediscover the baseDN later.

14377

The SmartPath AP AAA Server Settings profile did not prioritize user group-to-user profile mappings in the admin-defined order.

14360

Using a single quote (') in a SmartPath AP host name caused issues with the SmartPath EMS VMA GUI display when configuring an SSID.

14333

If you upgraded SmartPath EMS VMA to 4.0r1 with Configuration Rollback enabled in the Update CAPWAP Server Settings section on the SmartPath EMS VMA Services page, it was not possible to disable it.

14331

If you disabled DFS in a radio profile and pushed the configuration to a SmartPath AP, the configuration audit continued to show a mismatch between the SmartPath AP configuration stored on SmartPath EMS VMA and that running on the SmartPath AP.

13222

When a client had a bad health score (Monitor > Clients > Active Clients) and you refreshed it to make sure (Operation > Refresh Client), the client health score changed to 100 although the real score remained bad.

Federal Communication Commission Interference Statement

Each Black Box product described in this manual complies with part 15 of the FCC Rules when operating under the following restrictions: (1) This device may not cause harmful interference, and (2) they must accept any RF interference received, including interference that might cause an unwanted impact on their operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

Reorient or relocate the receiving antenna

Increase the separation between the equipment and receiver

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected

Consult the dealer or an experienced radio/TV technician for help

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment

Important: FCC Regulatory Warning Notices

LWN602A devices are restricted to indoor use due to their operation in 5 GHz frequencies, which are shared by mobile satellite systems and government radar systems. The FCC requires that these products only be used indoors to reduce the potential for harmful interference with co-channel radar that might be operating in the 5.25–5.35 or 5.47–5.725 GHz frequency ranges in the same area. The conflicting activity of radar stations and these devices can cause interference or damage to each other. In addition, these devices have a radar detection function that might interrupt normal operations when they detect a radar signal. To reduce the risk of interference even further, installing these devices away from windows is recommended.

LWN602A devices operating within the 5.15–5.25 GHz frequency range are restricted to indoor environments.

The FCC region code is set in the device during the manufacturing process, the option to set it to any region other than FCC is disabled, and the country code selection function has been completely removed from all U.S. models. It is impossible for the end user to change the region to anything other than FCC.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 23 centimeters (9 inches) between the radiator and your body.

The availability of some specific channel and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by end user.

Only attach antennas that are certified for use with this device. Replacing antennas with unauthorized, high-gain antennas greatly increases the risk of interference and invalidates the FCC certification.

Wi-Fi Certification

The Wi-Fi CERTIFIED™ Logo is a certification mark of the Wi-Fi Alliance®. The SmartPath APs have been certified for WPA™, WPA2™, WMM® (Wi-Fi Multimedia™), WMM Power Save, IEEE 802.11d, IEEE 802.11h, and the following types of EAP (Extensible Authentication Protocol):

- EAP-TLS
- EAP-SIM
- EAP-TTLS/MSCHAPv2
- EAP-AKA
- PEAPv0/EAP-MSCHAPv2
- EAP-FAST
- PEAPv1/EAP-GTC

The SmarPath APs (LWN602A and LWN602HA) have also been certified for short guard interval and 40-MHz operation in the 5-GHz band.

EC Conformance Declaration

CE

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

- EN 60950-1 (IEC 60950-1) - Product Safety
- EN 301 893 - Technical requirements for 5-GHz radio equipment
- EN 300 328 - Technical requirements for 2.4-GHz radio equipment
- EN 301 489-1 / EN 301 489-17 - EMC requirements for radio equipment

WEEE and RoHS Compliance

SmartPath products have been reviewed, analyzed, and found to be in compliance with the European Union (EU) directive for Waste Electrical and Electronic Equipment (WEEE) and with the EU directive for the Restriction of Hazardous Substances (RoHS).

Countries of Operation and Conditions of Use in the European Community

SmartPath APs are intended to be operated in all countries of the European Community. Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below.

- Before operating a SmartPath AP, the admin or installer must properly enter the current country code as described in Black Box product documentation.

NOTE: For U.S. model owners: To comply with U.S. FCC regulations, the country selection function has been completely removed from all U.S. models. The above function is for non-U.S. models only.

- SmartPath APs automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation might result in illegal operation and cause harmful interference to other systems. The admin is obligated to ensure SmartPath APs are operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this section.
- SmartPath APs can be operated indoors or outdoors in all countries of the European Community using the 2.4 GHz band: Channels 1–13, except where noted below:

– In Italy and Luxembourg, you must apply for a license from the national spectrum authority to operate a SmartPath AP outside your own premises and for public use or service.

– In Belgium outdoor operation is only permitted using the 2.46- to 2.4835-GHz band: Channel 13.

– In France outdoor operation is limited to the 2.454- to 2.4835-GHz band (Channels 8 to 13) at a maximum of 10 mW EIRP (effective isotropic radiated power).

– In Norway, the 2.4-GHz band cannot be used outdoors within a 20-km radius of the center of Ny-Ålesund.

– In Russia, the 2.4-GHz band is for indoor use only.

- Because radar systems use some bands in the 5-GHz spectrum, WLAN devices operating in these bands must use Dynamic Frequency Selection (DFS) to detect radar activity and switch channels automatically to avoid interfering with radar operations. For the ETSI region, the SmartPath AP (LWN602HA) is certified for the latest ETSI EN 301 893 v1.5.1 DFS requirements and can use DFS channels 52 to 140 (5.26 GHz to 5.32 GHz, and 5.5 GHz to 5.7 GHz). To comply with ETSI regulations when deploying a SmartPath AP (LWN602HA) device outdoors, set the 5-GHz radio to operate on the DFS channels and enable DFS. When deploying a SmartPath AP (LWN602HA) indoors, then the 5-GHz radio can also use Channels 36 to 48 as well as the DFS channels. The maximum transmit power for channels from 36 to 48 is 17 dBm in the ETSI region. Because this maximum is enforced by SmartPath OS, the SmartPath AP automatically limits the power to 17 dBm even if the setting is greater than that.
- The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at installation to match the intended destination. The firmware setting is accessible by the end user. Some national restrictions are noted below:

– In Italy and Luxembourg, you must apply for a license from the national spectrum authority to operate a SmartPath AP outside your own premises and for public use or service in the 5.15- to 5.35-GHz band (Channels 36 to 64) and 5.47- to 5.725-GHz band (Channels 100 to 140).

– In Russia, you can only use the 5.15- to 5.35-GHz band at 100 mW (20 dBm) indoors, in closed industrial and warehouse areas, and on-board aircraft for local network and crew communications during all stages of a flight and for public WLAN access only at an altitude of 3000 meters or higher. You can only use the 5.65- to 5.825-GHz band with 100 mW EIRP on board aircraft at an altitude of 3000 meters or higher.

Declaration of Conformity in Languages of the European Community

English: Hereby, we declare that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Finnish: Valmistaja Black Box vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Dutch: Hierbij verklaart Black Box dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. Bij deze Black Box dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.

French: Par la présente Black Box déclare que cet appareil Radio LAN est conforme aux exigences essentielles et aux autres dispositions relatives à la directive 1999/5/CE.

Swedish: Härmed intygar Black Box att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Danish: Undertegnede Black Box erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.

German: Hiermit erklärt Black Box, dass sich dieser/diese/ dieses Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi) Hiermit erklärt Black Box die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)

Italian: Con la presente Black Box dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Spanish: Por medio de la presente Black Box declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

Portuguese: Black Box declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

SmartPath AP Safety Compliance

Power Cord Safety

Please read the following safety information carefully before installing a SmartPath AP:

WARNING: Installation and removal of SmartPath APs must be carried out by qualified personnel only.

- SmartPath APs must be connected to a grounded (earthed) outlet to comply with international safety standards.
- Do not connect SmartPath APs to an AC outlet (power supply) without a ground (earth) connection.
- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN 60320/IEC320 appliance inlet.
- The socket outlet must be near the SmartPath AP and easily accessible. You can only remove power from a SmartPath AP by disconnecting the power cord from the outlet.
- SmartPath APs operate under Safety Extra-Low Voltage (SELV) conditions according to IEC 60950. The conditions are only maintained if the equipment to which they are connected also operates under SELV conditions.
- A SmartPath AP receiving power through its Power over Ethernet (PoE) interface must be in the same building as the equipment from which it receives power.

France and Peru only:

SmartPath APs cannot be powered from IT* supplies. If your supplies are of IT type, then a SmartPath AP must be powered by 230 V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labelled Neutral, connected directly to ground (earth). *Impédance à la terre

IMPORTANT: Before making connections, make sure you have the correct cord set. Check it (read the label on the cable) against the description in this section.

U.S.A. and Canada only:

- The cord set must be UL® and CSA certified.
- Minimum specifications for the flexible cord:

- No. 18 AWG, not longer than 2 m, or 16 AWG

- Type SV or SJ

- The cord set must have a rated current capacity of at least 10 A.

- The attachment plug must be an earth-grounding type with NEMA 5-15P (15 A, 125 V) or NEMA 6-15 (15 A, 250 V) configuration.

Denmark only:

- The supply plug must comply with Section 107-2-D1, Standard DK2-1a or DK2-5a.
- Switzerland:
- The supply plug must comply with SEV/ASE 1011.

U.K. only:

- The supply plug must comply with BS1363 (3-pin 13 A) and be fitted with a 5-A fuse that complies with BS1362.
- The power (mains) cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum).
- IEC-320 receptacle.

NOTES

Black Box Tech Support: FREE! Live. 24/7.

Great tech support is just 30 seconds away at 724-746-5500 or blackbox.com.

BLACK BOX®
NETWORK SERVICES

About Black Box

Black Box provides an extensive range of networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech Support available in 30 seconds or less.

© Copyright 2012. Black Box Corporation. All rights reserved.

Trademarks Used in this Manual

Black Box® and the Double Diamond logo are registered trademarks, and SmartPath is a trademark, of BB Technologies, Inc.

Apple and MacBookPro are registered trademarks of Apple Computer, Inc.

ASUS is a registered trademark of Asustek Computer, Inc.

Bonjour is a trademark of Bon Jour Group, L.P. Bon Jour Arkansas, Inc.

Cisco is a registered trademark of Cisco Technology, Inc.

Dell is a registered trademark of Dell, Inc.

Godex is a registered trademark of Godex International.

Intel is a registered trademark of Intel Corporation.

OmniTouch is a trademark of Alcatel-Lucent S.A.

Skype is a registered trademark of Skype Corporation.

SpectraLink is a registered trademark of SpectraLink Corporation.

Windows is a registered trademark of Microsoft Corporation.

Any third-party trademarks appearing in this document are acknowledged to be the property of their respective owners.